Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SE05/000039

International filing date: 17 January 2005 (17.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/536,491
Filing date: 15 January 2004 (15.01.2004)

Date of receipt at the International Bureau: 10 March 2005 (10.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1287814

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 28, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/536,491*
FILING DATE: *January 15, 2004*

SE/05/39

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

T Lawrence

T. LAWRENCE
Certifying Officer

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a r quest for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Express Mail Label No.

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Anders	Liden	

□ *Additional inventors are being named on the _____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

A TECHNIQUE FOR IPv4 MOBILITY FROM IPv6 NETWORKS

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ Customer Number 22907 → *Place Customer Number Bar Code Label here*

Type Customer Number here

OR

□ Firm *or* Individual Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS (*check all that apply*)

☒ Specification *Number of Pages* 52 □ CD(s), Number

☒ Drawing(s) *Number of Sheets* 2 □ Other (specify)

☒ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.

□ A check or money order is enclosed to cover the filing fees

□ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 19-0733

□ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) 80

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

□ Yes, the name of the U.S. Government agency and the Government contract number are: _____.

Respectfully submitted,

SIGNATURE Donald A Motte Reg No. 42,912 for

Date 01/15/04

TYPED or PRINTED NAME STEVEN P. SCHAD

REGISTRATION NO. (*if appropriate*) 32,550

Docket Number: 00254.00035

TELEPHONE 202 824 3195

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C., 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Unplugged

Strictly C nfidential Information

Author Anders Lidén	Document number IPU-2003:0458	Filename IPU_2003_0458_text
Approver	Date 2004-01-08	Revision PA1

A TECHNIQUE FOR IPv4 MOBILITY FROM IPv6 NETWORKS

1 FIELD OF THE INVENTION

The present invention relates to mobile data communication in general. More specifically, the present invention describes a technique for IPv4 mobility from IPv6 networks using Mobile IPv4 signalling sent over IPv6, together with a new Mobile IPv4 extension.

2 BACKGROUND AND SUMMARY OF THE INVENTION

The following definitions are introduced for the purpose of clarity.

FA Foreign Agent: The primary responsibility of an FA is to act a a tunnel agent which establishes a tunnel to a HA on behalf of a Mobile Node in mobile IPv4.

HA Home Agent: The primary responsibility of the HA is to act as a tunnel agent which terminates the Mobile IPv4 tunnel, and which encapsulates datagrams to be sent to the Mobile Node in Mobile IPv4.

IETF Internet Engineering Task Force: The IETF is the standardization organization for the Internet community.

IPv4 Internet Protocol version 4. IPv4 is a network layer protocol according to the ISO protocol layering. IPv4 is the major end-to-end protocol between Mobile and Fixed End-Systems for Data Communications.

IPv6 Internet Protocol version 6. IPv6 is a network layer protocol according to the ISO protocol layering. IPv6 is the next generation end-to-end protocol between Mobile and Fixed End-Systems for Data Communications.

MIPv4 Mobile IPv4: MIPv4 is an IPv4 mobility standard being defined by the IETF with the purpose to make IPv4 networks mobility aware, i.e. providing IPv4 entities knowledge on where a Mobile Node is attached to the network. The standard includes the definition of a Foreign Agent and a Home Agent.

MN Mobile Node: The MN comprises both the Terminal Equipment (TE) and the Mobile Termination (MT).

RFC Request For Comment: The collective name of standard documents produced within the IETF. Each standard document starts with RFC and a number, e.g. RFC3519 is th standard for Mobile IPv4 NAT traversal.

Mobile IPv4 is defining a Home Agent as the anchor point with which the Mobile Node always has a relationship, and a Foreign Agent, which acts as the local tunnel-endpoint at the access network where the Mobile Node is visiting. While moving from one IPv4 sub network to another, the Mobile Node point of attachment (FA) may change. At each point of attachment, mobile IPv4 either requires the availability of a standalone Foreign Agent or the usage of a co-located care-of address in the Mobile Node itself in the case that no Foreign Agent is available.

The present invention aims at providing a method for IPv4 mobility from IPv6 networks using Mobile IPv4 signalling together with a new Mobile IPv4 extension. The following references are also of general interest for the understanding of the present invention:

Perkins, Charlie; IP Mobility Support; RFC3344; http://www.ietf.org/rfc/rfc3344.txt; August 2002

Tsirtsis, G. and P. Srisuresh; Network Address Translation – Protocol Translation (NAT-PT); RFC2766; http://www.ietf.org/rfc/rfc2766.txt; February 2000

H. Levkowetz and S. Vaarala; Mobile IP Traversal of Network Address Translation (NAT) Devices; RFC3519; http://www.ietf.org/rfc/rfc3519.txt; May 2003

3 SUMMARY OF INVENTION

The following invention describes a technique for IPv4 mobility from IPv6 networks, using Mobile IPv4 signalling sent over IPv6, together with a new Mobile IPv4 extension.

4 BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features, and advantages of the invention will be apparent from the following description of preferred example embodiments as well as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout.

Fig. 1 is a flow chart diagram showing a Mobile Node registering from an IPv6 network or returning to the home network.

Fig. 2 is a flow chart diagram showing a Mobile Node registering from an IPv6 network configured with a NAT-PT gateway or returning to the hom network.

5 DETAILED DESCRIPTION OF THE DRAWINGS

In the following description, for the purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats, techniques, etc. in order to provide a thorough understanding of the present invention. Although specific protocols are referred to for the purpose of facilitation the description, the present invention is not necessarily limited to such specific protocols. However, it will be apparent to one skilled in the art that the present Invention may be practiced in other embodiments that depart from these specific details. In other instances, detail description of well-known methods, devices, and circuits are omitted so as not to obscure the description.of the present invention under unnecessary detail.

The present invention provides a technique for IPv4 mobility from IPv6 networks, using Mobile IPv4 signalling messages that are sent over IPv6. In this technique a new Mobile IPv4 extension is used to hold the IPv6 care-of address of the Mobile Node in the Registration Request.

Figure 1 illustrates a Mobile Node 2 registering in a visited IPv6 network 5, in co-located mode. The Mobile Node will send a registration request to the Home Agent 1 over IPv6 with an extension containing the IPv6 care-of address for the Mobile Node. Upon receiving the registration request, the Home Agent will use the IPv6 address in the extension as the end-point of the IPv4 over IPv6 tunnel that is set up from the Home Agent to the Mobile Node.

Figure 2 illustrates a Mobile Node 2 registering in a visited IPv6 network 5 that is configured with a NAT-PT gateway 6, in co-located mode. The Mobile Node will lookup the IPv6 address of the Home Agent from the DNSv6 server 7. When the IPv6 address is received from the DNSv6 server, the Mobile Node will send a registration request to the Home Agent 1 over IPv6 with an extension containing the IPv6 care-of address for the Mobile Node. The packet containing the registration request will be translated from IPv6 to IPv4 in the NAT-PT gateway and sent over IPv4 to the Home Agent. Upon receiving the registration request, the Home Agent will use the source address of the registration request as the end-point of the IPv4 UDP tunn l.

6 DESCRIPTION OF THE INVENTION

The first situation described is when the Home Agent is configured with an IPv6 address and when a Mobile Node registers co-located from a visited IPv6 network. The Mobile Node has aquired an IPv6 address in th Visited IPv6 network, how this is done is out of the scope of this pat nt application. The Mobile Node will then send a registration request

Author Anders Lidén	Document number IPU-2003:0458	Filename IPU_2003_0458_text
Approver	Date 2004-01-08	Revision PA1

to its Home Agent over IPv6 with an extension containing the IPv6 care-of address of the Mobile Node. The care-of address field in the registration request is set to zero. When the Home Agent receive the registration request it will use the IPv6 address in the IPv6 care-of address extension as the tunnel end-point address when setting up IPv4 over IPv6 tunneling to the Mobile Node. How the IPv4 over IPv6 tunneling is set up is outside the scope of this patent application. When tunneling has been set up, the Home Agent will send back a registration reply to the Mobile Node over IPv6.

The second situation described is when the Home Agent is configured with an IPv4 address and a Mobile Node registers co-located from a visited IPv6 network that is configured with a NAT-PT gateway. The Mobile Node has aquired an IPv6 address in the visited IPv6 network, how this is done is cut of the scope of this patent application. Before the Mobile Node send a registration request it will first have to do a DNS lookup from the local DNSv6 server for the IPv6 address of the Home Agent. The returned IPv6 address will contain the IPv4 address of the Home Agent as described in the NAT-PT RFC 2766. The Mobile Node will then send a registration request to the IPv6 address retrieved from the DNS server, together with an extension containing the IPv6 care-of address of the Mobile Node. The packet containing the registration request will be translated from IPv6 to IPv4 in the NAT-PT gateway, and sent to the IPv4 address of the Home Agent. When the The Home Agent will authenticate the Mobile Node and as the care-of address field is set to zero in the registration request, the Home Agent will set up UDP tunneling to the source IPv4 address in the registration request, as defined in the NAT traversal RFC 3519. When UDP tunneling has been set up, the Home Agent will send back a registration reply to the source IPv4 address in the registration request. The packet containing the registration reply will be translated from IPv4 to IPv6 in the NAT-PT gateway and sent to the IPv6 address of the Mobile Node.

If a Mobile Node moves from an IPv6 network to its home IPv4 network it will de-register from the Home Agent. Upon receiving a de-registration request the Home Agent will remove the binding entry for the home address of the Mobile Node and stop tunneling to the Mobile Node.

Fig 1

1. Home agent
2. Mobile Node
3. Home Network
4. IPv6 Internet
5. Visited IPv6 network

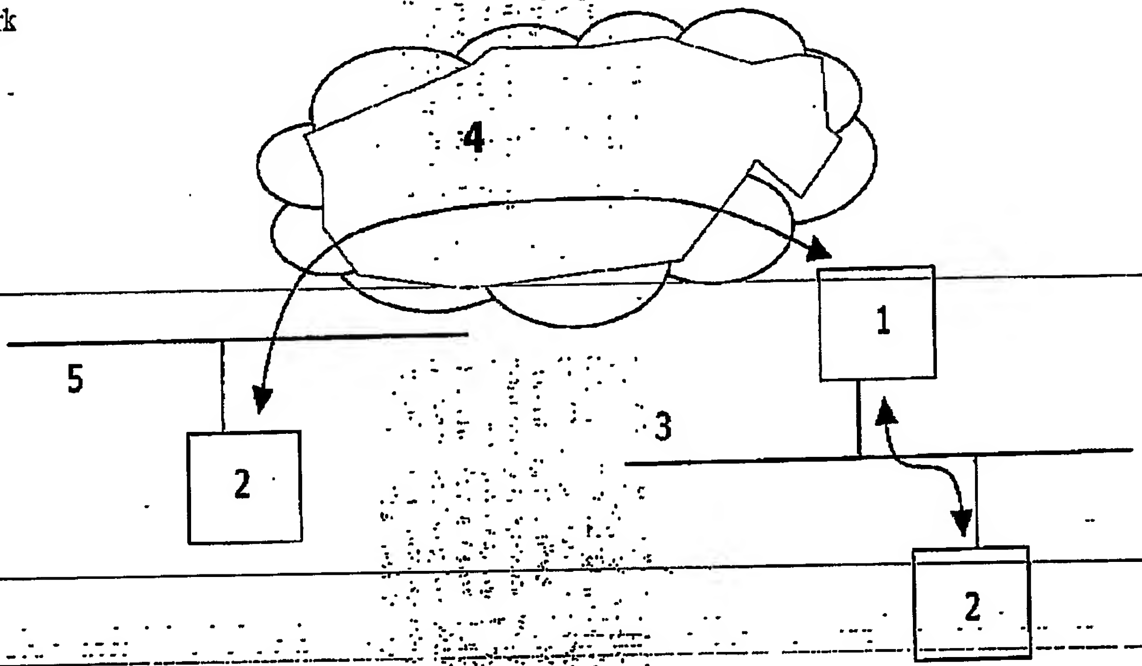
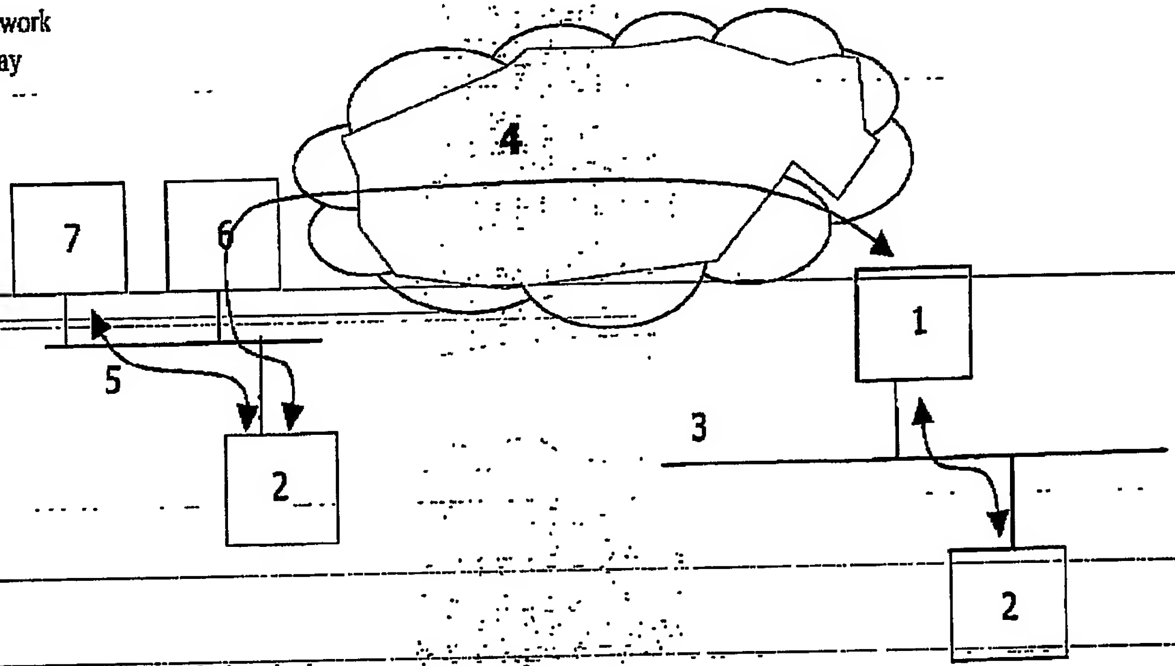


Fig 2

1. Home agent
2. Mobile Node
3. Home Network
4. IPv4 Internet
5. Visited IPv6 network
6. NAT-PT Gateway
7. DNSv6 Server



Seamless Mobility Between Current and Future IP Networks

Anders Lidén

January 1, 2004

Master Thesis
Department of Computer Science and Electrical Engineering
Division of Computer Communication
Luleå University of Technology

Abstract

During the last few years 3G cellular networks are starting to be deployed, but it is not until the next generation of cellular networks, 4G, that the data transfer rates are high enough to motivate users to be mobile at all times. 4G networks will probably transfer data and voice over the next generation Internet Protocol, IPv6, due to the massive amount of IP devices predicted to be used around the world. Mobile users can today use Mobile IPv4 from cellular access networks to connect their laptop or handheld device securely to the home network to use internal services, but Mobile IPv4 cannot be used to deliver IPv4 mobility from IPv6 access networks.

The purpose of the work presented in this thesis is to propose and implement a solution for Mobile IPv4 that allow mobile users to roam seamlessly between access networks that are using different versions of the Internet Protocol, while maintaining a secured IPv4 connection to the home network. In the theoretical part the proposed solution is presented, how it works and why it is needed. Other mechanisms that are available are discussed and together they are combined into a complete solution that can deliver IPv4 and IPv6 mobility from any access network.

The proposed solution developed during this thesis is implemented as a prototype in ipUnplugged's Roaming Gateway and Roaming Client products to demonstrate how the solution can be used. To test the implementation a combined IPv4/IPv6 test network is set up in a controlled lab environment. In the theoretical evaluation the functionality, performance and usability of the solution is analyzed.

Contents

Preface

The work leading to this master thesis was performed during the autumn 2003 at ipUnplugged AB in Stockholm, Sweden. This master thesis concludes the author's Master of Science education in Computer Science and Engineering at Luleå University of Technology.

Purpose and goal

The main object of the work behind this thesis is to investigate how the transition from networks using the current Internet protocol to networks using the next generation Internet protocol can be done as efficiently and transparently as possible for mobile users. Currently the focus of current methods are mostly on stationary users, but the transition is more complicated for mobile users because of their behavior, i.e. they are moving between networks that may use different versions of the Internet Protocol. For instance, a mobile user can connect to an IPv4 network at the office, but when the user leaves the office and travels by train to a customer meeting, the only Internet access available may be through a cellular phone service running on IPv6. How can mobile users make sure that they can seamlessly and securely access their home networks regardless of the Internet Protocol used in access networks?

IP Unplugged is a developer of Mobile IP-based networking products which enable mobile users to seamlessly and securely access their home networks from any network including LANs, wireless LANs and 3G (GPRS, UMTS and CDMA2000). Currently ipUnplugged's products support IPv4 networks, but the goal of this thesis is to propose and implement a prototype of a solution that allows users of ipUnplugged's solution to seamlessly and securely access their home networks regardless of the Internet protocol used in access networks.

Demarcations

The solution presented in this thesis is not an IETF [IETF] standard and there is no Internet draft that describe the method used. The solution developed during this master thesis is an ipUnplugged proprietary solution.

Organization of this thesis

The thesis is organized as follows:

- Chapter 1 – Introduction. Here is the current and next generation Internet protocol presented, as well as the mobile user behavior and the problems associated with the next generation Internet protocol for mobile users.

- Chapter 2 – Transition to the Next Generation Internet Protocol. This chapter presents the details of IPv6 and discusses the transition to IPv6 and the methods available to make the transition as smooth as possible.
- Chapter 3 – Mobility Between IPv4 and IPv6 Networks. Here is mobility between different networks discussed and a new extension to Mobile IPv4 is presented as a solution for seamless IPv4 mobility when moving between IPv4 and IPv6 access networks.
- Chapter 4 – Mobile IPv4 over IPv6. This chapter describes the details of the new solution for Mobile IPv4 that was developed during this master thesis.
- Chapter 5 – Implementation. Here is the implementation process of the new Mobile IPv4 solution described.
- Chapter 6 – Evaluation. This chapter evaluates the implementation of the Mobile IPv4 over IPv6 solution in ipUnplugged's products.
- Chapter 7 – Conclusion. This chapter concludes the master thesis and presents work experiences and conclusions.

Acknowledgements

I would like to thank my supervisor Hans Sjöstrand at ipUnplugged AB, and examiner Andreas Jonsson at Luleå University of Technology for their advice and support. I thank all people at ipUnplugged AB for making the everyday work more pleasant and joyful and I would especially like to acknowledge Peter Larsson and Erik Lidén for their technical advice and support during the prototype implementation.

Chapter 1

Introduction

Internet is the largest network in existence, and it is constantly growing. The massive number of IP devices that are predicted to be used around the world in the near future has brought forward the need for a revision of the currently used Internet protocol as the currently used protocol is not expected to cope with the needs of the future.

1.1 An Internet Briefing

Internet is a large global network that consist a vast amount of interconnected networks. The networks are interconnected through routers, which basically are computers with several networks attached to them. The task of the router is to send data between the different networks. The routers together with an addressing system and a transport protocol, called the Internet Protocol [IPv4], makes it possible for an arbitrary computer to reach any other computer attached to the Internet. If a router along the path to the destination would fail, there are mechanisms that may find another way to the destination if possible. This means that all computers connected to the Internet has to use the same addressing system in order to send data among each other.

During the last few years, the number of IP devices connected to the Internet has virtually exploded and due to the allocation mechanism that is used to allocate addresses in the Internet Protocol, some parts of the world are beginning to run out of addresses. A new version of the Internet Protocol called IPv6 [IPv6] has been defined that solves the address shortage problem as well as other problems with the currently used Internet Protocol. The new protocol is however not backwards compatible, and it is therefore hard to deploy in the Internet.

1.2 Mobile Users

Mobile users are different from stationary users in the way that they often move between different networks to connect to the Internet. A normal day for a mobile user may start at the office, connected to the local network either via LAN or wireless LAN. In this environment the user can access the necessary services, such as Intranet, mail server, file storage etc. When the mobile user leaves the office and takes the train to meet a customer, the user may use a cellular phone service to connect to the Internet to send a mail or get some documents. In order for the mobile user to use the services normally available in the office, a mobile VPN is needed. Mobile IP [MIPv4] is a protocol that makes it possible for mobile users to maintain their IP address in their home network, while connected to other access networks outside of the home network. This will make it possible for the mobile user to access services that are only available in the home network. However, the possibility to access services that are usually only available in the home network introduces security issues. The Mobile IP standard does not define how to secure the traffic, this is why a separate security mechanism is needed, IPsec [IPsec] for example. Mobile IP with IPsec can deliver a secure seamless mobility solution to a mobile user. Access networks, such as GPRS, CDMA2000 and UMTS today use IPv4 as the network protocol, but in the near future cellular phone services are likely to use IPv6 as network protocol as IPv6 uses a large address space, suitable for the large predicted amount of mobile devices running on IP such as cellular phones and band-held computers. To use Mobile IP for seamless mobility while running IPv4 applications, it is today required to be connected to an IPv4 access network.

1.3 Problem Statement

Today almost every access network uses IPv4 as its network protocol, it is mostly in experimental networks that IPv6 is used. However, it is likely that IPv6 will be used in the next generation of cellular networks. One example is the experimental 4G cellular network that NTT DoCoMo is working on [DoCoMo], which uses IPv6 as network protocol.

In order to deploy IPv6 in access networks, it is important that end users do not need to reconfigure their computers whenever they connect to an IPv6 access network and that they can reach services that are available in the IPv4 Internet. This is why several transition mechanisms have been developed that can be used to make the transition to IPv6 as smooth as possible. For example, by using an IPv6 capable web browser and a transition mechanisms that translate IPv6 traffic to IPv4 traffic makes it possible to reach IPv4 services on the Internet from an IPv6 access network. But as most applications today only support IPv4 there is a need to still be able to run IPv4 applications when connected to an IPv6 access network. This is especially true when it comes to mobile users that want the possibility to securely connect to their home network to reach IPv4 services. Mobile IP solves this problem when the user is connected to an IPv4 access network, but when IPv6 access networks are being deployed, Mobile IP cannot deliver IPv4 mobility from these access networks. This is why there is a need for a solution that can deliver IPv4 mobility from IPv6 access networks. How can this be done in a way that does not introduce unnecessary investments in IPv6 infrastructure?

1.4 Thesis Solution

The work presented in this thesis is a proposal and implementation of a solution for Mobile IPv4 that allow mobile users to move freely between access networks that are using different versions of the Internet Protocol, while maintaining a secure IPv4 connection to the home network. Other solutions that can solve the problem presented in the problem statement are also discussed and together they can be combined to a complete mobility solution for both IPv4 and IPv6 mobility.

Chapter 2

Transition to the Next Generation Internet Protocol

Before trying to solve the problem introduced in the problem statement, it is necessary to know what has already been achieved in this area. This chapter begins with a presentation of the currently used Internet Protocol and the new successor IPv6. In this chapter mechanisms that can be used to make the transition to the next generation Internet Protocol as smooth as possible are also discussed.

2.1 The Current Internet Protocol

The current Internet Protocol, IPv4, was standardized in ARPANET RFC 791 in 1981 [IPv4]. IPv4 has been the most successful network protocol ever deployed. Considering it was one of the first network protocols, the durability of IPv4 has been better than expected. Today, however, with the growth of the Internet, the development of a global business environment built upon the Internet and the advances in technology, IPv4 threatens to hold back the technical flexibility of the Internet.

2.1.1 Address Space

IPv4 has a 32-bit address space that allows for 2^32 or 4,294,967,296 possible addresses. In the late 1970's when the IPv4 address space was designed it was unimaginable that it could be exhausted. However, due to changes in technology and an allocation practise that did not anticipate the recent growth of hosts on the Internet, the IPv4 address space was consumed to the point that by 1992 it was clear that a replacement protocol would be needed. In a world where all computers are connected to the Internet and when the future world looks to be full of new devices that will be connected to the global network, like portable phones, PDAs, Internet appliances, vehicles etc, there is simply not enough addresses to go around. IPv4's usable life has been extended via a technology called Network Address Translation (NAT) [NAT], which is a clever mechanism that conserves scarce IPv4 addresses. Essentially, NAT allows enterprises to deploy potentially large networks using shared IP-addressing space, 10.0.0.0 or 192.168.0.0 for example, and translating their Internet-bound traffic at their network edge to unique addresses assigned to their enterprise. In this way, an enterprise can deploy a thousand of computers and reserve few unique IP addresses. NAT is effective in that way that it allows more nodes to join the network than would be possible if all nodes required routable addresses. This capability comes with a cost, the loss of end-to-end communication, which advanced applications often require. Many applications today requires advanced workarounds to traverse NAT gateways, which creates unnecessary technically complicated architectures.

2.2 The Next Generation Internet Protocol

The next generation Internet Protocol is called IPv6. It uses 128 bit addresses, which is four times larger than an IPv4 address. With IPv6 it is hard to conceive that the IPv6 address space with its 2^128 addresses will ever be consumed. The relatively large size of the IPv6 address is designed to be subdivided into hierarchal routing domains that reflect the topology of the modern Internet. The 128 bit address provide multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing, which is currently lacking on the IPv4-based Internet. The architecture of IPv6 is described in RFC 2373 [IPv6].

2.2.1 Header Changes in IPv6

Since the IPv6 addresses are four times larger than IPv4 addresses, the format of the IPv6 header had to be changed. This change allowed the designers of the protocol to redesign the header from scratch and make it better than its predecessor. The IPv4 header contains fields that have been discarded in the IPv6 header, as shown in figure 2.1.

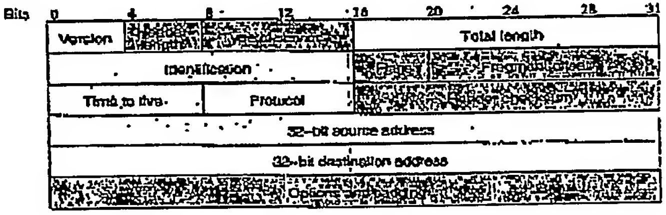


Figure 2.1: The IPv4 header format.

The header format has been simplified in IPv6, the shaded fields in figure 2.1 does not exist in IPv6, as shown in figure 2.2. Despite that, the IPv6 header is still twice as large as the IPv4 header. The IPv4 header length is 20 bytes without options, to be compared to the IPv6 header length which is 40 bytes. One of the important changes is that there is no options field in the IPv6 header. In IPv4 the options field can be used to add information about various optional services, for example information related to encryption. Because of this, the IPv4 header length can vary depending on the situation. Due to this difference in length, routers that control communications according to the information in the IPv4 header can't assume that the IPv4 header size is fixed, which makes it difficult to speed up packet processing with hardware assist. In IPv6, information related to additional services is moved to an extension header, in that case the type of extension header is stored in the next header field. The IPv6 header in figure 2.2 is called basic header, this means that for plain packets the length of an IPv6 header is fixed to 40 bytes which makes it easier to speed up packet processing with hardware assist.

Another field that exist in figure 2.1 but not in figure 2.2 is the Header Checksum field. A header checksum is calculated using the numbers in the header and it is

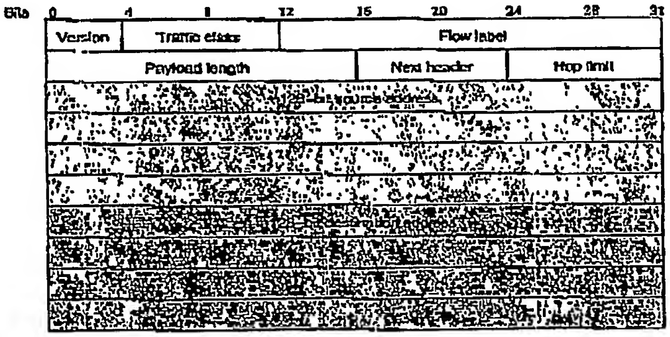


Figure 2.2: The IPv6 header format.

used to check for errors in the header information. The problem with this approach is that the header contains a field called Time To Live, which changes every time the packet goes through a router. This means that the Header Checksum has to be recalculated every time the packet goes through a router. If we could free up routers from calculations like these, the delay could be reduced. Actually, the transport layer header, TCP or UDP for instance, also has a Header Checksum field which checks for errors in various information, including the source and destination addresses in the IP header. Since performing the same calculations at the IP layer is redundant and unnecessary, Header Checksum is removed from IPv6.

The 8-bit "Type of Service" field in figure 2.1 may be used by networks to define the handling of the datagram during transport, for example the priority of the datagram. IPv6 provides the same function with a field called Traffic Class.

The Flow Label field in figure 2.2 is of 20-bit length and is a field newly established for IPv6. By using this field, the packet's sender or intermediate devices can specify a series of packets, such as Voice over IP, as a flow, and request particular service for this flow. Some IPv4 devices are equipped with the ability to recognize traffic flow and assign particular priority to each flow. However, these devices are required to not only check IP layer information, they also has to check the port number which is information that belongs to a higher layer. The Flow Label field attempts to put together all necessary information and provide them at the IP layer. However, specifics on how to use it is still undecided.

To conclude, IPv6 aims to provide an intelligent transmission framework that is easy to handle for intermediate devices by keeping the basic header simple and fixed in length.

2.3 Transition Mechanisms

The next generation Internet Protocol is not backwards compatible with the current Internet Protocol, this makes it hard to deploy the next generation Internet Protocol as old applications will no longer work. In order to make the transition to IPv6 as trouble free as possible, a number of transition mechanisms have been defined. The following is a brief overview of some of the transition mechanisms that the ngtrans IETF working group [ngtrans] is working on. A few of them are already IETF proposed standards, RFCs, while others are still Internet drafts.

2.3.1 IETF Proposed Standards

Connection of IPv6 Domains via IPv4 Clouds (6to4)

The 6to4 transition mechanism is an IETF standard and specified in RFC 3056 [6to4]. This transition mechanism is normally used when one IPv6 network needs to be connected to another IPv6 network as it provides a way to connect IPv6 end-site networks by automatic tunneling over the intervening IPv4 Internet. A special IPv6 routing prefix (2002::/16) is used to indicate that the remaining 32-bits of the external routing prefix contains the IPv4 end-point address of a boundary IPv6 router for that site that will respond to IPv6 in IPv4 encapsulation. This will allow a host that is located behind a 6to4 router to communicate with other 6to4 hosts on the Internet. When the host sends an IPv6 packet to another 6to4 host, the packet is tunneled in IPv4 at the 6to4 router using the IPv4 address contained in the prefix of the 6to4 destination address as the IPv4 destination address. At the destination site the IPv4 header is removed at the 6to4 boundary router and forwarded to the appropriate 6to4 host by using the IPv6 routing infrastructure of the destination site.

By using a 6to4 replay router, a 6to4 host can send IPv6 packets to a native IPv6 node on the IPv6 Internet. The packets are encapsulated in IPv4 at the 6to4 router and sent to the IPv4 address of the configured 6to4 relay router. The relay router has native connectivity to the IPv4 and IPv6 Internet. The 6to4 relay router removes the IPv4 header and forwards the IPv6 packet to the appropriate IPv6 Internet host.

Network Address Translation - Protocol Translation (NAT-PT)

NAT-PT is a standards track IETF RFC [NAT-PT] describing an IPv6/IPv4 translator. NAT-PT allows native IPv6 hosts and applications to communicate with native IPv4 hosts and applications, and vice versa. A NAT-PT device resides at the boundary between an IPv6 and IPv4 network. Each NAT-PT device retains a pool of globally routable IPv4 addresses, which are used to assign to IPv6 nodes on a dynamic basis as sessions are initiated across the IPv6/IPv4 boundary. In addition to address translation, header translation is performed as described in the SIIT mechanism [SIIT]. As opposed to SIIT, which is a stateless translation mechanism, NAT-PT retains state via the IPv4- to-IPv6 address mappings which are retained for the duration of each session. NAT-PT can be extended to NAPT-PT (Network Address Port Translation - Protocol Translation). NAPT-PT takes the address translation a stage further by enabling the translation of port numbers as well. This makes it possible to re-use one IPv4 pool address and map this one IPv4 address to many IPv6 hosts. The basic NAT-PT translation device may additionally contain ALG:s (Application Level Gateways). ALG:s are necessary when IP addresses are embedded within the payload of an IP packet. For normal packet translation, NAT-PT would not look within the payload for IP addresses. Typical protocols that embed IP addresses in the payload are FTP and DNS. NAT-PT requires no special configuration on the client, apart from using the correct DNS server which can be configured automatically through DHCPv6 for example.

Stateless IP/ICMP Translator (SIIT)

SIIT [SIIT] is a transition mechanism algorithm that translates between IPv4 and IPv6 packet headers, including ICMP, in separate translator "boxes" in the network, without requiring any per-connection state in those "boxes". This algorithm can be used as a part of a solution that allows IPv6 hosts, which do not have a permanently assigned IPv4 address, to communicate with IPv4-only hosts. NAT-PT is an example of such a solution. The RFC neither specifies how to do address assignment nor routing to and from the IPv6 hosts when they communicate with IPv4-only hosts.

IPv6-to-IPv4 Transport Relay Translator (TRT)

The IPv6-to-IPv4 Transport Relay Translator (TRT) [TRT] works in a way that is similar to the NAT-PT mechanism. The difference is that the TCP connection from an IPv6 node to an IPv4 node is intercepted in the TRT. For example, when a TCP packet from the IPv6 node destined to the IPv4 node is received at the TRT, the TRT sets up a new TCP connection to the IPv4 node and forwards the data in the packets from the IPv6 node. This means that two TCP connections are set up for every TCP session.

Dual Stack Hosts Using "Bump-in-the-API" (BIA)

The BIA mechanism [BIA] inserts an API translator between the socket API module and the TCP/IP module in the dual stack hosts, to translate the IPv4 socket API function to IPv6 socket API function and vice versa. This allows the transition to be simplified without IP header translation. When using BIA, the dual stack host assumes that there exists both IPv4 and IPv6 stacks on the local node. When an application on the dual stack communicate with other IPv6 hosts, the API translator detects the socket API functions from IPv4 applications and invokes the IPv6 socket API functions to communicate with the IPv6 hosts, and vice versa. In order to support communication between IPv4 applications and the target IPv6 hosts, pooled IPv4 addresses will be assigned through the name resolver in the API translator.

2.3.2 IETF Internet Drafts

Dual Stack Transition Mechanism (DSTM)

The dual stack transition mechanism [DSTM] is based on the use of IPv4-over-IPv6 tunnels to carry IPv4 traffic within an IPv6 dominant network and provides a method to allocate a temporary IPv4 address to Dual IP Layer IPv6/IPv4 capable nodes. DSTM is also a way to avoid the use of NAT-PT for communication with IPv4-only nodes and applications. When DSTM is deployed in a network, an IPv4 address can be allocated to a Dual IP Layer IPv6/IPv4 capable node to connect with IPv4-only nodes and applications, without modification to any IPv4-only node or application, or the IPv4 application on the DSTM node. This allocation mechanism is coupled with the ability to perform IPv4-over-IPv6 tunneling of IPv4 packets inside the IPv6-dominant network. The DSTM mechanism consist of a DSTM server and DSTM capable nodes. The DSTM server is responsible for IPv4 address allocation to client nodes and may also provide tunnel endpoints to the DSTM nodes. The DSTM nodes will use tunnel end points to tunnel IPv4 packets inside IPv6 to a DSTM Border router. The DSTM border router then decapsulates the IPv6 packets and transmits the IPv4 packets to the destination IPv4 node. The DSTM border router will have to cache the path back to the DSTM node for the IPv4 address to tunnel the packet in IPv6 to the original DSTM node.

Dual Stack Mobile IPv4

The dual stack Mobile IPv4 draft [Dual-MIPv4] provides IPv6 extensions to the Mobile IPv4 protocol. The extensions allow a node that has IPv4 and IPv6 addresses to maintain communications with either or both of its addresses while moving in IPv4 or dual stack networks. The specification essentially separates the Mobile IP signaling version from the IP version of the traffic that it tunnels. Mobile IPv4 with these new extensions becomes a signaling protocol that runs over IPv4, and yet can set-up any combination of IPv4 and/or IPv6 over IPv4 tunnels. However, this method cannot be used when the user moves to an IPv6 only access network as the signaling is only sent over IPv4.

Dual Stack Mobile IPv6

The dual stack Mobile IPv6 draft [Dual-MIPv6] provides IPv4 extensions to the Mobile IPv6 protocol [MIPv6]. The extensions allow a node that has IPv4 and IPv6 addresses to roam within the Internet using Mobile IPv6 only, while simultaneously maintaining connections using their IPv4 and IPv6 home addresses. When the mobile user is located on a dual stack or IPv6 only access network, the Mobile IPv6 signaling is sent over IPv6 to the Home Agent. When the mobile user is located on an IPv4 only access network, the Mobile IPv6 signaling packets are tunneled in IPv4 to the Home Agent. The drawback with the dual stack Mobile IPv6 mechanism is that it does not handle situations when only private IPv4 addresses are available in the access network, which is a common situation.

IPv6 over Mobile IPv4

IPv6 over Mobile IPv4 [IPv6-MIPv4] specifies a Mobile IPv4 extension that may be used by dual stack mobile nodes to obtain IPv6 service with the use of a Mobile IPv4 registration. This extension allows for immediate deployment of IPv6 on dual stack mobile devices, without the need for a full IPv6 infrastructure. It is believed that providing IPv6 services to mobile devices in the short term will spur the growth of IPv6 networks. The specification requires that the mobile node and Home Agent have dual IPv4 and IPv6 stacks, but there are no changes to the FA and it does not need to be dual stack. By using this mechanism together with MIPv6, IPv6 mobility can be achieved from any access network.

Chapter 3

Mobility Between IPv4 and IPv6 Networks

This chapter introduces a possible solution to the problem with mobility between IPv4 and IPv6 networks. It begins by pointing out some issues that are important to take into account when trying to solve this problem.

3.1 Overview

In a perfect world, it is possible to introduce new network protocols and mechanisms only by a small software upgrade. But taking into account the massive amount of networks deployed in the Internet and the even greater amount of users it is not hard to realize that such an approach is not possible. The deployment of IPv6 is a good example of how hard it can be to introduce something new when so many people and computers are affected by the change. The reason why IPv6 is likely to be used in the next generation of cellular networks is the massive amount of devices that are predicted to be used in these networks in the future, all over the world. There is simply not enough IPv4 addresses to go around. When it comes to mobility, solutions exist today for both IPv4 and IPv6, but these solutions do not solve the problem with a mixed network environment, which is likely to be common once the access networks start to use IPv6. The existing mobility solutions will be presented below as it is necessary to understand how they work in order to solve the problems with mobility between IPv4 and IPv6 networks.

3.2 Existing Solutions for IP Mobility

The existing mobility standards for IPv4 and IPv6 will be described briefly to give the reader an understanding of the two protocols.

3.2.1 Mobile IPv4

In general, on the Internet, IP packets are transported from their source to their destination by allowing routers to forward data packets from incoming network interfaces to outbound network interfaces according to information obtained via routing protocols. Routing tables typically maintain the next-hop information for each destination IP network. The IP address of a packet normally specifies the IP client's point of attachment to the network, which means that the IP address has to change at a new point of attachment. To alter the routing of IP packets intended for a mobile client to the new point of attachment requires a new IP address associated with that new point of attachment. However, to maintain existing transport protocol layer connections as the client moves, the mobile client's IP address must remain the same.

Mobile IP solves this problem by introducing two new functional entities within IP networks. Those are the Foreign Agent, FA and the Home Agent, HA. The two new entities together with enhancements in the Mobile Node (client), are the basic building blocks for a Mobile IP enabled network. The last entity needed to provide a full reference for a basic Mobile IP enabled network is the Correspondent Node, CN. The Correspondent Node is another IP entity, for example an Internet Server with which the Mobile Node communicates. The Correspondent Node does not need to have any Mobile IP knowledge at all, but the Mobile Node needs upgrading and new functions are required in the visiting and home networks.

Mobile IP works by allowing the Mobile Node to be associated with two IP addresses, the "home" address and the "care-of" address. The home address remains fixed, while the care-of address changes at each new point of attachment to the Internet. The home IP address assigned to the Mobile Node makes it appear as if the Mobile Node is attached to its home network. This is the IP address where the Mobile Node seems to be reachable for other Internet clients and services. From the view of the Correspondent Node, the Mobile Node seems to be attached to the home network independently of which network it is currently visiting.

A mobile agent, the Home Agent, that is provided in a home network receives traffic that is directed to the Mobile Node's home IP address even when the Mobile Node is not physically attached to the home network. When the Mobile Node is attached to a foreign network, a Home Agent tunnels that traffic to a Foreign Agent using the Mobile Node's current care-of address. The care-of address identifies the Mobile Node's current topological point of attachment to the Internet, this is why the care-of address can be used to tunnel packets to the Mobile Node. If the Mobile Node is attached to the home network, the Home Agent simply arranges to have the data traffic delivered to the Mobile Node's point of attachment in the home network. Whenever the Mobile Node moves its point of attachment, it registers a new care-of address with its Home Agent.

When the Mobile Node is attached to a foreign network, packets sent from the Mobile Node can be sent directly to the Correspondent Node. This is called triangular routing which has one problem: as many routers filters out packets with source addresses that are inconsistent with their routing table (so called ingress filtering), private addressing cannot be immediately used when visiting a foreign network. The solution to this problem is a technique called reverse tunneling, which means that the Foreign Agent also tunnels packets from the Mobile Node back to the Home Agent instead of directly sending them to the Correspondent Node.

At each access network, a Mobile IP client normally requires a stand-alone Foreign Agent. However, if the access network in question does not provide a Foreign Agent service then it is possible to include a Co-located care-of address in the Mobile Node. The care-of address is the temporary address in the visited access network to which the Home Agent forwards incoming packets and vice versa. The two different ways of getting the mobile node associated with a Mobile IP care-of address, network based Foreign Agent versus Co-located care-of address, has somewhat different characteristics.

When a network based Foreign Agent is used, the Mobile IP tunnel is terminated at the Foreign Agent in the network. On the other hand, when using Co-located care-of addresses, the tunnel is terminated in the Mobile Node. This means that when the access network is the bottleneck, network based Foreign Agents are more efficient since there is no extra overhead for the tunneling on the access network.

A network based Foreign Agent care-of address is shared between several visiting mobile nodes. Packets to the Mobile Node are intercepted by the Home Agent and tunneled to the Foreign Agent in the visited network. The Foreign Agent decapsulates the packets and forwards them to the Mobile Node. Since Foreign Agents can handle many mobile nodes with one single care-of address, network based Foreign Agents does not require the visited network to have a large IP address space made available.

When using a Co-located care-of address, the Mobile Node is associated with a unique care-of address. The Mobile IP tunnel from the Home Agent is extended and terminated in the Mobile Nod itself. In this case there is no need for a Foreign Agent in the visited network, which means that the visited network does not need to be Mobile IP aware. Co-located care-of address requires one unique care-of address in the visited network per visited Mobile Node.

The two control messages used in Mobile IP are Registration Request and Registration Reply which are sent in UDP packets. The Registration Request message is used to register the Mobile Node's current care-of address with its Home Agent. A Registration Reply is sent back to the Mobile Node, notifying if the registration was successful or not. The control messages are described in detail as it is necessary to know how they are defined in order to understand how the protocol can be extended to support IPv4 mobility from IPv6 access networks as described in chapter 4.

Registration Request

The Registration Request that is sent from a Mobile Node to the Home Agent is specified to hold various addresses, identification and control bits, as well as extensions used for authentication of users. The format of the Registration Request is as shown in figure 3.1.

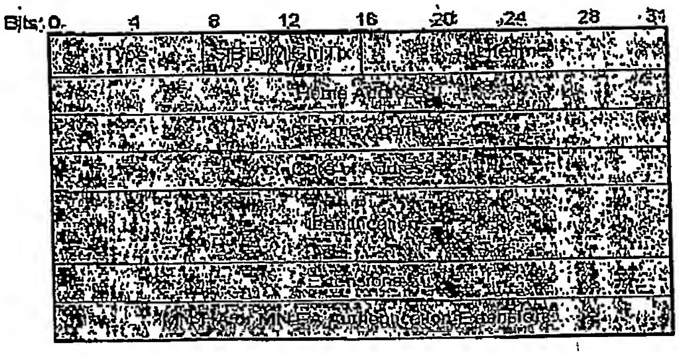


Figure 3.1: The Registration Request format.

The Registration Request is sent in a UDP packet with a variable source port and a destination port set to 434. The values used in the Registration Request fields are specified in the RFC as follows:

Type 1 (Registration Request)

S Simultaneous bindings. If the 'S' bit is set, the mobile node is requesting that the home agent retain its prior mobility bindings.

B	Broadcast datagrams. If the 'B' bit is set, the mobile node requests that the home agent tunnel to it any broadcast datagrams that it receives on the home network.
D	Decapsulation by mobile node. If the 'D' bit is set, the mobile node will itself decapsulate datagrams which are sent to the care-of address. That is, the mobile node is using a co-located care-of address.
M	Minimal encapsulation. If the 'M' bit is set, the mobile node requests that its home agent use minimal encapsulation for datagrams tunneled to the mobile node.
G	GRE encapsulation. If the 'G' bit is set, the mobile node requests that its home agent use GRE encapsulation for datagrams tunneled to the mobile node.
r	Sent as zero; ignored on reception. SHOULD NOT be allocated for any other uses.
T	Reverse Tunneling requested.
x	Sent as zero; ignored on reception.

Lifetime
The number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

Home Address
The IP address of the mobile node.

Home Agent
The IP address of the mobile node's home agent.

Care-of Address
The IP address for the end of the tunnel.

Identification
A 64-bit number, constructed by the mobile node, used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages.

Extensions
The fixed portion of the Registration Request is followed by one or more extension. An authorization-enabling extension MUST be included in all Registration Requests.

Registration Reply

The Registration Reply sent from the Home Agent to the Mobile Node is used to inform the Mobile Node if the registration was successful or not. The format of the Registration Request is as shown in figure 3.2.

The Registration Reply is sent in a UDP packet with source port 434 and a destination port set to the source port found in the corresponding Registration Request. The values used in the Registration Reply fields are specified in the RFC as follows:

Type 3 (Registration Reply)

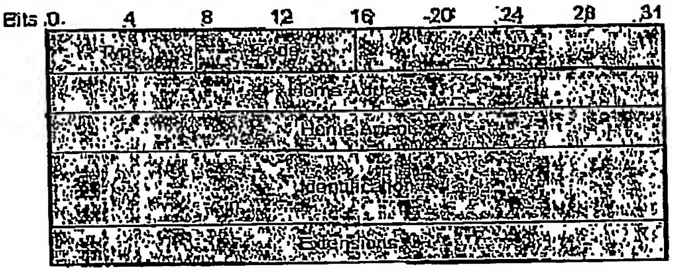


Figure 3.2: The Registration Reply format.

Code A value indicating the result of the Registration Request. See [MIPv4] for details.

Lifetime
If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Home Address
The IP address of the mobile node.

Home Agent
The IP address of the mobile node's home agent.

Identification
A 64-bit number used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages. The value is based on the Identification field from the Registration Request message from the mobile node, and on the style of replay protection used in the security context between the mobile node and its home agent (defined by the mobility security association between them, and SPI value in the authorization-enabling extension).

Extensions
The fixed portion of the Registration Reply is followed by one or more extension. An authorization-enabling extension MUST be included in all Registration Replies returned by the home agent.

3.2.2 Mobile IPv6

Mobile IPv6 is based on the concepts of Mobile IPv4, but as Mobile IPv6 is a part of the IPv6 standard the protocol is more integrated into IPv6, which makes it possible to introduce route optimization. There is no Foreign Agent in Mobile IPv6, this is due to new functionality in IPv6 where IPv6 Neighbor Discovery and Address Autoconfiguration allow hosts to operate in any location without any special support.

Mobile IPv6 extends IPv6 by introducing new destination options to IPv6. The new options are Binding Update, Binding Acknowledgement and Home Address option. The destination options are equivalent to the registration messages of Mobile

IPv4, except the Binding Request and Home Address option. However, because the options are carried in the destination options extension header of IPv6, the options can be piggybacked with any outgoing datagram with correct destination instead of having to send a separate UDP packet.

In Mobile IPv6 route optimization is a mandatory part of the protocol. Correspondent nodes have binding caches that contain the current valid bindings that the node is aware of. Each time a Correspondent Node is about to send a datagram, it first checks if it has a binding for the destination. If the binding exist, the node attaches a routing header with a single route segment to the datagram, sets the IPv6 destination address to the care-of address indicated by the binding and sets the original destination address to the route segment within the routing header. When the datagram arrives at the receiving Mobile Node, the Mobile Node detects the routing header and sends the packet onward to the address indicated in the routing header. Because the address is local to the Mobile Node, the packet is not actually sent but looped back to the Mobile Node, as the destination address is the Mobile Node's home address.

By using source routing and binding caches, Mobile IPv6 allows the correspondent nodes to communicate directly to the mobile nodes, avoiding triangular routing.

3.3 Mobility Between Different Networks

The problem of maintaining mobility between different access networks can be solved in a number of ways.. If we concentrate on the problem described in the problem statement, where a mobile user want the possibility to maintain IPv4 mobility while roaming between IPv4 and IPv6 access networks. This problem can be solved by using a mechanism described in chapter 2, called "Dual Stack Mobile IPv6" where the Mobile Node registers over IPv6 with the Home Agent, and by using new extensions it is possible to transfer IPv4 traffic in the IPv6 tunnel as well as IPv6 traffic. This solution is quite elegant, as it solves the problem of IPv4 mobility from IPv6 access networks, and it even allows the user to use IPv6 mobility as well. When the user moves from the IPv6 access network to an IPv4 access network, Mobile IPv4 is used as normal for IPv4 mobility. However, this solution has one major drawback, if IPv6 services are used and IPv6 networks are deployed in home networks, this solution would have been perfect, but this is currently not the case in many networks. Companies that have invested money in mobility solutions for IPv4 and only use IPv4 in the home network are not likely going to invest even more money in infrastructure for IPv6 mobility, just to be able to use IPv6 access networks to maintain IPv4 mobility. It is unlikely that vendors of Mobile IPv4 solutions are going to include Mobile IPv6 support in their Mobile IPv4 solutions to solve such a problem, as it is going to need a large implementation effort in order to introduce Mobile IPv6 support. Instead there is a need for a more simple solution that can quite easily be introduced as a part of a Mobile IPv4 solution, at a sensible implementation cost. This is why the Mobile IPv4 over IPv6 solution has been developed during this master thesis. It does not require the mobile user to be aware of the network protocol used in the access network, and it is relatively easy to implement for Mobile IP vendors.

3.3.1 Mobile IPv4 over IPv6

The proposed way to solve the problem of running IPv4 applications when attached to IPv6 access networks is to extend Mobile IPv4 with the possibility to register over IPv6. The method has been named Mobile IPv4 over IPv6, as it is essentially

Mobile IPv4 that is transported over IPv6. There exists a few prerequisites in order to use Mobile IPv4 over IPv6:

1. The Home Agent must be configured with a globally routable IPv6 address.

2. The IPv6 access network must use stateless or stateful address auto-configuration, or possibly DHCPv6.

3. The Mobile Node needs to know the IPv6 address of the Home Agent.

A Mobile Node that is attached to an IPv6 access network, can configure itself with an IPv6 address using stateless or stateful address auto-configuration, or possibly DHCPv6. When the Mobile Node notice that it is attached to an IPv6 network, it sends a Mobile IPv4 Registration Request in an IPv6 UDP datagram to the IPv6 address of the Home Agent. The Home Agent sets up IPv6 tunneling towards the Mobile Node and sends a Registration Reply back to the Mobile Node. For this to work, a new Mobile IPv4 extension needs to be defined that can store the IPv6 Care-of address of the Mobile Node as the care-of address field in the Registration Request is too small. This extension is attached to the Registration Request that is sent to the Home Agent.

This solution will allow the mobile user to run IPv4 applications while attached to an IPv6 access network. It even allows the Mobile IPv4 user to seamlessly roam between IPv4 and IPv6 access networks, which means that a mobile user that is running IPv4 applications does not need to be aware of the Internet protocol used in the access network. The Mobile IPv4 over IPv6 solution is described in detail in chapter 4, and the implementation of this solution performed during the master thesis is described in chapter 5.

3.3.2 IPv6 over Mobile IPv4

Mobile IPv4 over IPv6 solved the situation when the home network of a mobile user is running IPv4 and the mobile user wants to run IPv4 applications, while being away from the home network. If the home network is running IPv6, Mobile IPv6 can be used to allow the mobile user to run IPv6 applications, but Mobile IPv6 can only be used when attached to an IPv6 access network. If the user is attached to an IPv4 access network, Mobile IPv6 services won't be available. One solution to solve this is to use IPv6 over Mobile IPv4, as specified in [Dual-MIPv4]. This requires that the home network is dual stack as the registration is done using the IPv4 home address for the Mobile user. The registration request is extended with an IPv6 address extension which the Mobile Node can use to request usage of the IPv6 home address, or an assigned dynamic IPv6 address. The Home Agent responds with a registration reply where the IPv6 address extension contains the IPv6 address to use.

3.4 The Complete Mobility Solution

If the home network of a mobile user is running IPv4 and IPv6 services on the same network, mobile users will need to be dual stack configured. In order to reach all services in the mixed environment of the home network, while outside the premises and away from the home network, a complete mobility solution for IPv4 and IPv6 mobility needs to be set up.

3.4.1 Combined Mobile IPv4 and Mobile IPv6 Solution

By combining the methods discussed in this thesis, it is possible to set up a complete solution for IPv4 and IPv6 mobility. In this environment, Mobile Nodes will have to be dual stack and Home Agents for Mobile IPv4 and IPv6 has to be set up in the home network. When the mobile user moves out from the corporate premises and connect to an access network, via a cellular phone service, wireless LAN or LAN for instance, the user should be able to register with its Home Agent, either via IPv4, IPv6 or both in order to achieve mobility for both IPv4 and IPv6. There are a number of different ways the mobile user can achieve mobility depending on the type of access network used. By combining the mechanisms in in figure 3.3 in different ways, IPv4 and IPv6 mobility can be achieved from any access network.

[illegible]	[illegible]
[illegible]	An IETF proposed standard, specified in RFC 3344.
[illegible]	An IETF Internet draft named "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt. Soon to become an IETF proposed standard.
[illegible]	A personal draft named "Dual Stack Mobile IPv4", draft-tsirtsis-dsmip-dsmipv4-00.txt
[illegible]	A personal draft named "Dual Stack Mobile IPv6", draft-tsirtsis-v4v6-mipv6-00.txt
[illegible]	A proprietary mechanism, implemented during this master thesis.

Figure 3.3: Table showing the mechanisms used for a combined environment.

The table in figure 3.4 illustrates the possible types of attachment to access networks, and which of the mechanisms that can be combined to achieve mobility in these access networks.

[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	MIPv4	IPv6 over MIPv4	MIPv4 + IPv6 over MIPv4
[illegible]	MIPv4 over IPv6 or IPv4 over MIPv6	MIPv6	MIPv4 over IPv6 + MIPv6 or IPv4 over MIPv6 + MIPv6
[illegible]	MIPv4	MIPv6	MIPv4 + MIPv6 or MIPv4 + IPv6 over MIPv4 or MIPv6 + IPv4 over MIPv6 or MIPv6 + MIPv4 over IPv6

Figure 3.4: Mobility from all access networks.

As can be seen in the table in figure 3.4, there are two ways to achieve mobility for IPv4 when attached to an IPv6 access network. One is IPv4 over MIPv6, but as this requires a full Mobile IPv6 implementation as well as IPv4 over Mobile IPv6 implementation in the Mobile Node and Home Agent. The Mobile IPv4 over IPv6 mechanism that has been developed during this master thesis has been designed to take advantage of the currently available implementations of Mobile IPv4. From a dual stack access network, there are numerous ways to achieve IPv4 and IPv6 mobility, but the most attractive of them is probably to use Mobile IPv4 and Mobile IPv6 separately as this allows the use of separate mobility solutions for IPv4 and IPv6. On the other hand, if fast hand over times are essential, for voice over IP usage for instance, a combined solution that only requires one registration might be more attractive.

3.4.2 Deployment Scenarios

The Mobile IPv4 over IPv6 solution can be deployed as shown in figure 3.5 where the Home Agent is accessible from the IPv4 and IPv6 Internet. A deployment like this allow mobile nodes to securely access IPv4 services in the home network from IPv4 and IPv6 access networks.

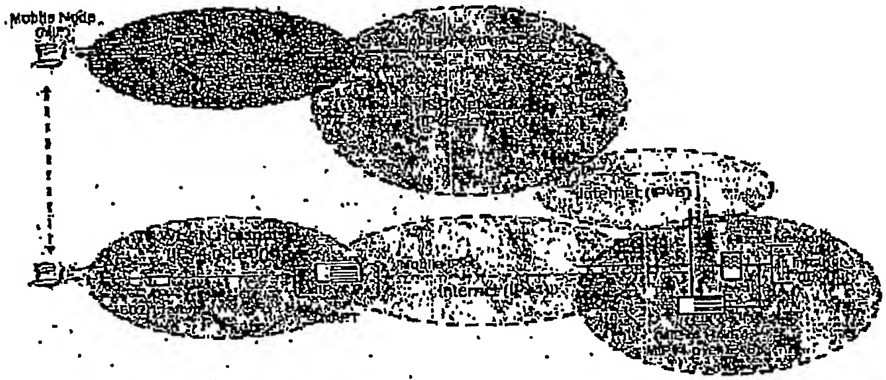


Figure 3.5: Mobile IPv4 over IPv6 deployment scenario.

The complete mobility solution for IPv4 and IPv6 can be deployed as shown in figure 3.6. In this deployment scenario Mobile IPv4 and the dual stack mobile IPv4 solution [Dual-MIPv4], is used when the Mobile Node is located on an IPv4 access network. When the Mobile Node is located on an IPv6 access network, Mobile IPv6 is used together with the dual stack mobile IPv6 solution [Dual-MIPv6].

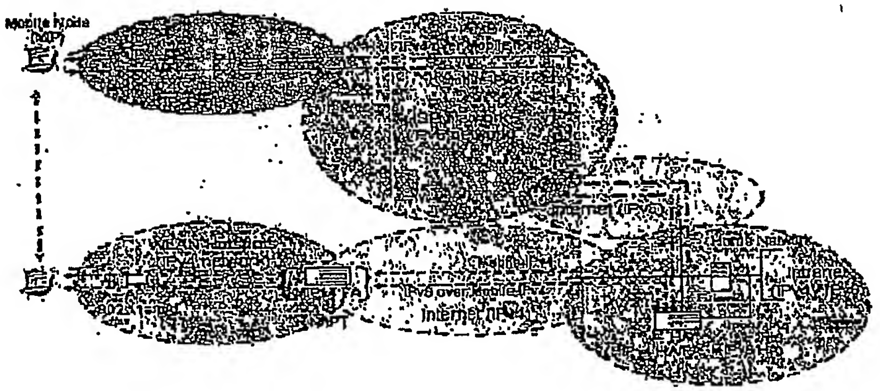


Figure 3.0: Deployment scenario for one of the possible combined mobility solutions for IPv4 and IPv6 mobility from any access network.

Chapter 4

Mobile IPv4 over IPv6

4.1 Background

The commercial use of IPv6 is very limited today mostly due to the lack of support for IPv6 in commercial applications. For this reason IPv6 will most likely first be deployed in access networks and operator backbones, for instance a cellular phone service running on IPv6. Therefore a new Mobile IPv4 extension and method to use Mobile IPv4 over IPv6 networks has been developed, which allow mobile users to connect to their IPv4 home network in a secure way, while seamlessly roaming between IPv4 and IPv6 access networks.

4.2 Extending Mobile IPv4 with IPv6 Functionality

4.2.1 Overview

In order for the Mobile Node to be able to register Co-Located with the Home Agent over IPv6, the Home Agent has to be configured with a globally routable IPv6 address and the Mobile Node has to acquire an IPv6 care-of address. When these conditions are met, the Mobile Node can register Co-Located over IPv6, but the Home Agent has to be able to obtain the care-of address of the Mobile Node. It is not sufficient for the Home Agent to obtain the care-of address by looking at the source address in the Registration Request since the packet could have been manipulated on the way to the Home Agent by a man-in-the-middle attack. Instead it is necessary to define a new extension to the Registration Request to transport the care-of address of the Mobile Node. This new extension can then be secured by the MN-HA Authentication Extension at the end of the Registration Request. It is therefore important that the new extension is located before the MN-HA Authentication Extension in the Registration Request. When the Home Agent has acquired the care-of Address of the Mobile Node and authenticated the Mobile Node, it can set up an IPv6 tunnel towards the Mobile Node instead of the normal IPv4 tunnel. Using this method avoids the use of double tunnels, which would be the case if Mobile IPv4 was to be tunneled inside an IPv6 tunnel. The method of using a single IPv4 in IPv6 tunnel significantly decreases the overhead.

4.2.2 Deployment Scenario

When using Mobile IPv4 with the new extension, the mobile node can seamlessly roam between the different access networks as shown in figure 4.1. If the mobile node is connected to an IPv6 access network, the mobile node will configure itself with an IPv6 Care-of Address, using for instance Stateless Address Auto-configuration [RFC2462]. The mobile node can then register co-located over IPv6 with the Home Agent by sending Registration Requests over IPv6 with the new extension attached. This requires that the Home Agent is configured with a globally routable IPv6 address. Section 4.3 describes the details of the new extension used in co-located registration over IPv6.

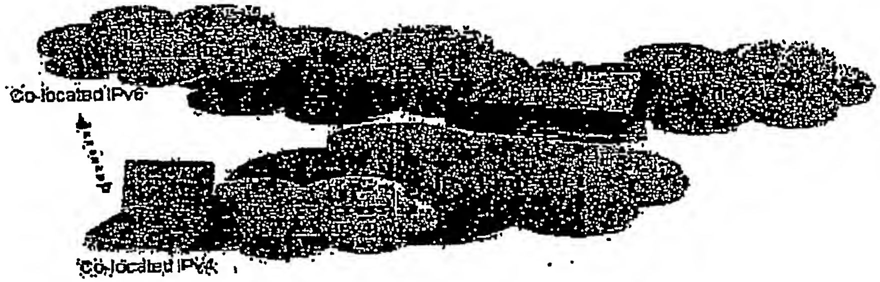


Figure 4.1: Deployment scenario where the new extension to Mobile IPv4 can be useful.

It is possible that the provider of the IPv6 access network is supplying its customers with a NAT-PT service [NAT-PT], which allows users on the IPv6 access network to communicate with IPv4 hosts on the Internet. Co-located registration through a NAT-PT router can also be supported if the Mobile Node and Home Agent is capable of NAPT traversal [RFC3519]. Section 4.3.3 describes how the mobile node can register through a NAT-PT gateway. If the mobile node is connected to a pure IPv4 network, the Mobile Node operates as normal without the new extension.

4.3 Extension Details

4.3.1 IPv6 Care-of Address Extension

The new extension to Mobile IPv4 that is used to carry the IPv6 care-of address of the Mobile Node is named "IPv6 Care-of Address Extension" from now on. If the IPv6 Care-of Address Extension is used, the bits of the care-of Address field in the Registration Request header must be set to zero. The IPv6 Care-of Address Extension should be attached to the Registration Requests before the MN-HA Authentication Extension so that it is secured from man-in-the-middle attacks.

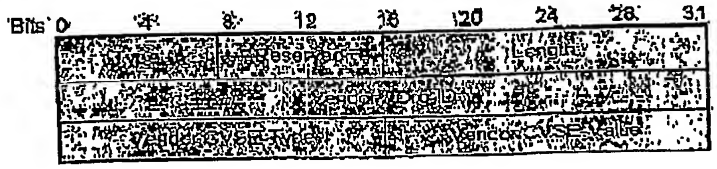


Figure 4.2: Format of the Critical Vendor Specific Extension.

The IPv6 Care-of Address extension is a Critical Vendor/Organization Specific Extension (CVSE) [RFC3115] displayed in figure 4.2. Below is the fields of the Critical Vendor Specific Extension described.

Type CVSE-TYPE-NUMBER 38

Reserved Reserved for future use. MUST be set to 0 on sending, MUST be ignored on reception.

Length Length in bytes of this extension, not including the Type and Length bytes.

Vendor/Org-ID
The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers RFC.

Vendor-CVSE-Type
Indicates the particular type of Vendor-CVSE-Extension. The administration of the Vendor-CVSE-Types is done by the Vendor.

Vendor-CVSE-Value
Vendor/organization specific data of this Vendor-CVSE-Extension. The Vendor-CVSE-Value is zero or more octets. The length of this field can be computed from the Length Field Value.

If the receiver does not recognize the extension, the entire packet is to be silently dropped. The IPv6 Care-of Address Extension has the length field set to 22 and the Vendor-CVSE-Value must be set to the 128-bit IPv6 care-of address assigned to the Mobile Node.

4.3.2 Co-Located registration over IPv6

When the Mobile Node is located on an IPv6 access network and has acquired an IPv6 address, it can register Co-Located with the Home Agent.

Mobile Node Actions

The Mobile Node has to be aware of the globally routable IPv6 address of the Home Agent. When the Mobile Node notice that it is connected to an IPv6 network and has configured a unique IPv6 address, it will try to send a Registration Request with the new IPv6 Care-of Address Extension towards the IPv6 address of the Home Agent. When a "registration accepted"-reply is received from the Home Agent, the Mobile Node can set up an IPv6 tunnel towards the Home Agent. All IPv4 traffic generated by the Mobile Node will be encapsulated in the IPv6 tunnel and sent towards the Home Agent.

Home Agent Actions

If the Home Agent is configured with a globally routable IPv6 address, it will listen to UDP port 434 over IPv6. When a Registration Request is received, the Home Agent checks if the IPv6 Care-of Address Extension is present in the Registration Request, if this is the case then the care-of address field must be zero. If the care-of address field is not set to zero, the Home Agent will send a "registration denied" Registration Reply to the Home Agent, and not allow the Mobile Node to register. On the other hand, if the care-of address field is set to zero, the Home Agent will authenticate the Mobile Node as usual. If the authentication is successful, the Home Agent will set up an IPv6 tunnel towards the IPv6 care-of address found in the IPv6 Care-of Address Extension. Finally the Home Agent will send a "registration accepted" Registration Reply to the Mobile Node.

4.3.3 Co-Located Registration over IPv6 Through NAT-PT

If the provider of the IPv6 access network is supplying its customers with a NAT-PT [NAT-PT] service, it is not necessary to configure the Home Agent with a globally routable IPv6 address, since the Registration Request sent over IPv6 can be translated by the NAT-PT gateway and sent over IPv4 to the Home Agent. This however require that the Mobile Node does a DNS lookup of the domain name of the Home Agent, and not use the IP address directly. If the access network is configured with a NAT-PT gateway, the DNS lookup will return the IPv6 address of the Home Agent if the domain name, and the Home Agent, is configured with a globally routable IPv6 address. In this case the registration procedure will be exactly the same as in section 4.3.2. On the other hand, if the domain name, and the Home Agent are only configured with a globally routable IPv4 address, the DNS lookup will return a faked IPv6 address with the IPv4 address embedded. When the Registration Request is sent towards this faked IPv6 address, the packet is translated in the NAT-PT gateway and sent towards the IPv4 address embedded in the IPv6 address the Registration Request was sent to.

For all this to work, the Mobile Node and Home Agent has to support NAPT traversal [RFC3519]. This means that when the Home Agent receives the Registration Request it checks if the address in the care-of address field in the Registration Request is different than that of the source address in the IP header. When used together with the IPv6 Care-of Address Extension, the Care-of Address field in the Registration Request is set to zero, thus it is different than the address in the source address field in the IP header. This means that NAT traversal should be activated and all traffic should be UDP encapsulated.

Chapter 5

Implementation

5.1 Introduction

During this master thesis, Mobile IPv4 over IPv6 was implemented in ipUnplugged's mobility solution. The solution consist of three products:

1. Roaming Gateway - Acts as a Home Agent and Foreign Agent in a network.
2. Roaming Client - The Mobile Node implementation on Microsoft Windows 2000/XP, to be installed on every mobile device that needs mobility.
3. Roaming Server - A web-based central management server used for central user and configuration management.

As Mobile IP does not define how to secure the traffic, an additional security mechanism is needed. IpUnplugged has chosen to use IPsec inside the Mobile IP tunnel to secure the traffic.

5.2 Goals

The goals of the implementation was to get a working prototype that could demonstrate how IPv4 mobility, secured with IPsec, could be maintained while roaming between IPv4 and IPv6 access networks. As the implementation was to be done by one person the project had to be demarcated to only include the necessary functionality in order to get a working prototype. For this prototype changes had to be made in the Roaming Gateway and the Roaming Client. The Roaming Server is not needed for this prototype as the configuration of the Roaming Gateway and Client is assumed to be done manually.

5.2.1 Home Agent

The following are the goals set up for the functionality of the Home Agent (Roaming Gateway) implementation:

1. The Home Agent has to be extended to handle Registration Requests over IPv6.
2. The Home Agent has to be able to send Registration Replies to the Mobile Node over IPv6.
3. The Home Agent has to handle the new IPv6 Care-of Address Extension in Registration Requests.

4. The Home Agent has to be able to decapsulate IPv6 tunneled IPv4 packets from the Mobile Node.

5. The Home Agent has to be able to encapsulate IPv4 packets in the IPv6 tunnel.

All of the above goals has to met in order for the Mobile IPv4 over IPv6 solution to work correctly.

5.2.2 Mobile Node

For a working implementation of the Mobile IPv4 over IPv6 solution the Mobile Node (Roaming Client) has to be extended with the following functionality:

1. The Mobile Node has to be able to receive router advertisements with prefix information, in order to configure the IPv6 address to use. The IPv6 address has to be configured using the stateless address auto-configuration method [RFC2462].

2. The Mobile Node has to be able to send Registration Requests over IPv6, using the configured IPv6 address as source address, and the Home Agent IPv6 address as destination address.

3. The Mobile Node has to be able to include the IPv6 Care-of Address Extension in the Registration Request.

4. The Mobile Node has to be able to tunnel IPv4 packets in IPv6 headers, destined for the Home Agent.

5. The Mobile Node has to be able to decapsulate IPv6 tunneled IPv4 packets from the Home Agent.

6. The Mobile Node has to be able split tunnel IPv6 traffic, i.e. IPv6 traffic should be sent directly out on the interface and not tunneled to the Home Agent. This allows the use of IPv6 services at the same time as IPv4 mobility is used from an IPv6 access network.

In order to use Mobile IPv4 over IPv6 without the need to install the IPv6 stack in Microsoft Windows 2000/XP, additional goals have been set up for optional implementation.

1. The Mobile Node should be able to notify the network interface driver to receive the necessary multicast traffic in order to receive router advertisements and neighbor solicitations. This is something that the IPv6 driver normally does, but as IPv6 will not be installed, the Mobile Node's Mobile IP driver has to do it.

2. The Mobile Node should be able to respond to neighbor solicitations. In order for the Mobile Node to behave as an IPv6 node among other nodes in the network, the Mobile Node should fully support Neighbor Discovery, but for a minimal prototype implementation it is enough to respond to neighbor solicitations. Neighbor solicitations are sent as a query to get the MAC address of the node, if the Mobile Node does not respond to these solicitations, IPv6 packets from the IPv6 router in the network cannot be sent to the Mobile Node.

5.2.3 Solution

Combining all features specified in the above goals for the Home Agent and Mobile Node will result in a solution that allows a mobile user to get IPv4 mobility independent of the Internet protocol used in the access network. To enhance the solution even more, the mobile user may not even have to install IPv6 in order to use Mobile IPv4 over IPv6.

5.3 Target Platforms

The Roaming Gateway is based on OpenBSD, where the Mobile IP functionality is implemented in C in the kernel and a Mobile IP daemon running in userspace that is implemented in C/C++.

The Roaming Client is implemented as a software application on Windows 2000/XP, using a low level miniport driver for network communication, a Windows service for Mobile IP operations and a control application. During the installation of the client a virtual interface is installed that communicates with the driver and acts as the home interface, configured with the home IP address of the user. This makes sure that when the mobile user moves from the home network and connects to a different access network, the higher level applications will not be aware of the IP address change. The miniport driver is developed in C and the Windows service and control application are developed in C++.

5.4 Home Agent

5.4.1 Overview.

The Roaming Gateway is ipUnplugged's mobility router with Home Agent and Foreign Agent functionality. As the Mobile IPv4 over IPv6 solution only use the Home Agent, the Foreign Agent does not need to be extended with any new functionality. The Home Agent implementation consist of two parts, one userspace Mobile IP daemon and Mobile IP forwarding/tunneling in the kernel. The following additional features have to be included in order for the Roaming Gateway to support Mobile IPv4 over IPv6:

1. The Mobile IP daemon has to accept incoming Registration Requests on UDP port 434 over IPv6.
2. The Mobile IP daemon has to be able to parse out the care-of address from the new IPv6 Care-of Address Extension.
3. The data structures used in the Mobile IP daemon has to be extended to support both IPv4 and IPv6 addresses.
4. The Mobile IP daemon has to be able to send Registration Replies over IPv6 to Mobile Nodes.
5. The communication channel between the Mobile IP daemon and the kernel has to be extended to support both IPv4 and IPv6 addresses.
6. The kernel has to be able to set up tunneling of traffic sent to the home IP address of the Mobile Node to the current care-of address of the Mobile Node.
7. The kernel has to be able to encapsulate IPv4 packets to the home address of the Mobile Node in IPv6 and send them to the care-of address of the Mobile Node.

8. The kernel has to be able to decapsulate IPv6 tunneled IPv4 packets from the Mobile Node.

5.4.2 Userspace

The first part to be extended with Mobile IPv4 over IPv6 functionality was the Mobile IP daemon, as it could easily be tested by a small program that can send Registration Requests over IPv6 to verify the new functionality. The Mobile IP daemon normally accept incoming Registration Requests on UDP port 434 over IPv4. The daemon has been extended to listen on UDP port 434 over IPv6 as well, for reception of Registration Requests sent over IPv6. All data structures in the Mobile IP daemon that holds IP addresses used in the Home Agent binding, such as care-of address, Home Agent address etc, have been extended to support both IPv4 and IPv6 addresses. The data structures uses variables of type uint32 or sockaddr structs to store IPv4 addresses, but in order to support both IPv4 and IPv6 addresses, the sockaddr_storage struct had to be used, which is specifically designed to be protocol independent. This however required quite extensive changes in the old code as these data structures are used extensively throughout the code.

The care-of address of a Mobile Node that registers over IPv6 is retrieved from the IPv6 Care-of Address Extension in the Registration Request. When a Mobile Node registers over IPv6 and the IPv6 Care-of Address Extension is not present in the Registration Request, the Mobile Node is not allowed to register. If the extension is available and the care-of address field is set to zero, the user can be authenticated and the registration will be accepted. The Mobile IP daemon then transfers the binding information to the kernel to set up Mobile IP tunneling. The communication channel between the daemon and the kernel has been extended to support both IPv4 and IPv6 addresses that are used in the binding information.

5.4.3 Kernel

When the userspace implementation was done, the kernel part of the Mobile IP implementation was extended with the necessary functionality. The Mobile IP code in the kernel that set up Mobile IP tunneling according to the information retrieved from the Mobile IP daemon, had to be extended to set up IPv4 in IPv6 tunneling. As the Roaming Gateway is based on OpenBSD, most of the necessary code for IPv4 in IPv6 tunneling was already available and could be enabled by using the INET6 compile option. This made the implementation in the kernel pretty straightforward as the IPv6 code in the kernel is organized in the same way as for IPv4.

5.4.4 Testing and Debugging

The extended functionality in the Home Agent was verified by a small program that can send faked Registration Requests over IPv6 to the Home Agent. It was necessary to write this small test program as it was felt to be advantageous to have a working implementation on the Home Agent before any work was started on the Mobile Node implementation. It was verified that the Mobile IP daemon parsed the Registration Request correctly and found the new IPv6 Care-of Address Extension. The daemon sent the binding information down to the kernel and it could be verified that IPv4 in IPv6 tunneling was set up correctly. The actual tunneling of packets could be verified by sending packets to the home address of the Mobile Node from another computer. Using Ethereal [Ethereal], the tunneled packets could be tracked and verified as sent on the outgoing IPv6 network. It was however not verified that the kernel decapsulated incoming tunneled packets from the Mobile Node correctly as this required to much work to verify at this stage. No special debugging tools were used to debug the Mobile IP daemon, but kernel core dumps was used to debug the kernel implementation.

5.4.5 Conclusion

The implementation of the new Home Agent functionality was thought to be the easier part of the Mobile IPv4 over IPv6 implementation. This was proved to be correct as the implementation only took about 5 weeks to complete. An installation CD for the Home Agent was made to make it easier to install the prototype in demo systems. When installing the system from the CD, the necessary IPv6 enabled command line applications are included which are needed during configuration of the system.

5.5 Mobile Node

5.5.1 Overview

The Roaming Client which is ipUnplugged's Mobile Node implementation is divided into a low level miniport driver, a Mobile IP Windows service, a userspace control application and a virtual network adapter. The miniport driver intercept incoming packets such as Registration Replies, ARP messages and tunneled packets, and delivers the packets to a platform independent intercept library that decapsulatse and decrypts tunneled packets which then are sent up to the virtual adapter. The intercept library also answer ARP requests and send control packets such as Registration Replies and router advertisements up to the Mobile IP service. The following additions had to be included in the Roaming Client to support Mobile IPv4 over IPv6:

1. The driver has to intercept incoming IPv6 packets.
2. The driver has to register each physical interface twice with the intercept library. The intercept library will then believe that there are two virtual interfaces for each physical interface. One for IPv4 and one for IPv6. This allows independent operation of the two interfaces within the Mobile IP service, which handle the IPv6 interface just like any other interface card connected to the computer.
3. The driver has to deliver the relevant IPv6 packets to the intercept library for further processing.
4. The intercept library has to be able to recognize router advertisements and send them up to the Mobile IP service.
5. The intercept library has to be able to recognize neighbor solicitations and send them up to the Mobile IP service.
6. The intercept library has to be able to recognize Mobile IP Registration Replies sent over IPv6 and send them up to the Mobile IP service.
7. The Mobile IP service has to be able to configure the IPv6 Care-of address, using the prefix received in router advertisements.
8. The Mobile IP service has to be able to compose Registration Requests with an IPv6 header instead of IPv4, to be sent down to the driver for delivery.
9. The Mobile IP service has to be able to compose Neighbor Advertisements to send to solicitating nodes.

10. The control application has to be able to present the currently used IPv6 Care-of address and IPv6 address of the Home Agent for the user in the configuration dialog when Co-located on IPv6.

5.5.2 Driver

When a new interface is connected to the computer, the driver informs the intercept library of the new interface. However, for each physical interface, the driver keeps track of two different identities, one for reception of IPv4 packets and one for IPv6 packets. The driver informs the intercept library that two new interfaces are added for each physical interface, using these two identities. This allows the two virtual interfaces to be treated separately in the intercept library.

To be able to intercept IPv6 packets the driver has to make sure that it can receive router advertisements and neighbor solicitations. If the IPv6 stack is installed, Windows will make sure that the necessary multicast MAC addresses are added to the multicast address list in the network interface driver. However, when the network interface previously has been connected to an IPv4-only network and later connected to an IPv6 network, Windows does not seem to add the necessary multicast MAC addresses to the address list. The MAC addresses are added to the address list after a timeout that can be as long as 20 seconds, which makes the hand-over times from an IPv4 network to an IPv6 network terribly slow. This can be solved by having the Mobile-IP driver add the necessary multicast addresses to the address list. This will also allow usage of the Mobile IPv4 over IPv6 mechanism without any IPv6 stack installed in Windows. By having the driver add the necessary multicast addresses to the address list, the hand-over times was reduced to less than one second. When an IPv6 packet is intercepted, the driver passes the packet to the intercept library together with the IPv6 identity of the interface the packet was received on.

Intercept Library

The intercept library is a part of the driver, and it makes a decision whether to process incoming packets further, leave them to the Windows IPv4/IPv6 stack or delete them. Packets that are processed further can be Registration Replies, ARP messages, ICMP messages, tunneled packets etc. In order to be able to handle incoming router advertisements, the intercept library identifies router advertisements and checks if there is any prefix information available. If the router advertisement contains prefix information, the packet is sent up to the Mobile IP service for further processing. Neighbor solicitations and Registration Replies are also sent up for further processing. Tunneled packets from the Home Agent are decapsulated, decrypted and sent up to the virtual adapter.

The intercept library also handles outgoing packets. When an IPv4 packet is sent into the virtual adapter, the intercept library makes sure that the packet is encrypted and encapsulated in an IPv6 or IPv4 packet, depending on the currently used Care-of address, for delivery to the Home Agent.

5.5.3 Mobile IP service

The Mobile IP service is started when the control application is started. The service handles decision making processes such as which network to use when multiple networks are available, when and where to send Registration Requests etc.

The Mobile IP service has been extended to handle IPv6 interfaces. When an IPv6 care-of address can be configured on an IPv6 interface, the service makes sure to compose and send out a Registration Request to the Home Agent over IPv6 with the new IPv6 Care-of Address Extension attached. The returning Registration Reply is processed and if the registration is successful, the service notifies the driver to set up tunneling towards the Home Agent and IPsec encryption of the traffic. The Mobile IP service also handles incoming neighbor solicitations and sends out neighbor advertisements to the solicitating nodes. This is something that could have been done more efficient directly in the driver, however this was not done due to time constraints as it was easier to compose neighbor solicitations in the Mobile IP service.

5.5.4 Control Application

The control application is used to enable and disable the client, show connection information, handle network adapter priorities etc. The control application was extended with the possibility to show the currently used IPv6 Care-of address when registered Co-located on IPv6, and the IPv6 address of the Home Agent in the configuration dialog, as show in figure 5.1. It is also possible to get some information in the system logs, for example when the client has configured the IPv6 Care-of address and when the client has registered with the Home Agent over IPv6.

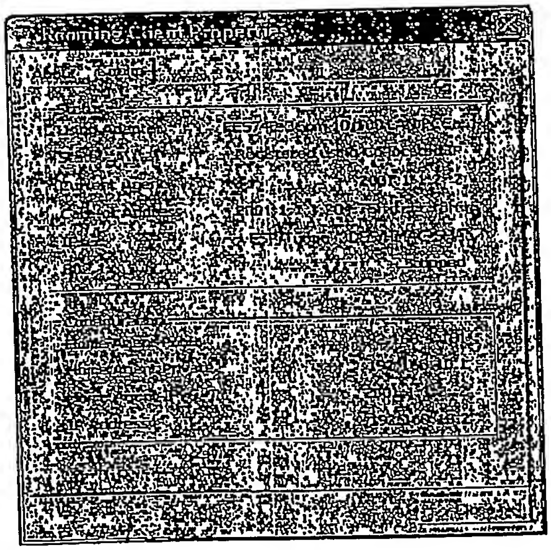


Figure 5.1: The configuration dialog in the Roaming Client.

5.5.5 Testing and Debugging

The client implementation could easily be tested against the Home Agent implementation. During testing it was found that the decapsulation of tunneled packets in the Home Agent did not work correctly, however this was corrected with a small fix.

Debugging of the Mobile IP driver was greatly simplified by the use of Compuware SoftICE debugger. Without a proper debugger for the driver it would have been very time consuming to implement the new functionality in the driver. The debugger in Microsoft Visual Studio .NET was used during development of the Mobile IP service application. Ethereal was used extensively during development to verify that packets sent to and from the Mobile Node were constructed correctly.

5.5.6 Conclusion

The implementation of the new Mobile Node functionality took about 10 weeks to complete. This implementation was seen to be the risky part of the project, but with good support from people at ipUnplugged, the new Mobile Node functionality was successfully implemented in the Roaming Client.

Chapter 6

Evaluation

6.1 Introduction

The evaluation of the implementation was done by verifying that the goals of the project was met. As the resulting implementation was set to be a prototype, only the necessary parts of the solution needed for a working prototype were tested and evaluated. Features of the solution that may have been affected by the code changes should be verified throughly when the prototype functionality is to be implemented in the final product.

6.2 Network Setup

The implementation was tested and evaluated in a local test environment. The test network was set up to allow testing of the client from four different types of networks, the home network, co-located on IPv4, co-located on IPv6 and co-located on a dual stack network. The resulting network setup is shown in figure 6.1. An additional Foreign Agent, accessible via wireless network was also used to verify functionality from a foreign IPv4 network.

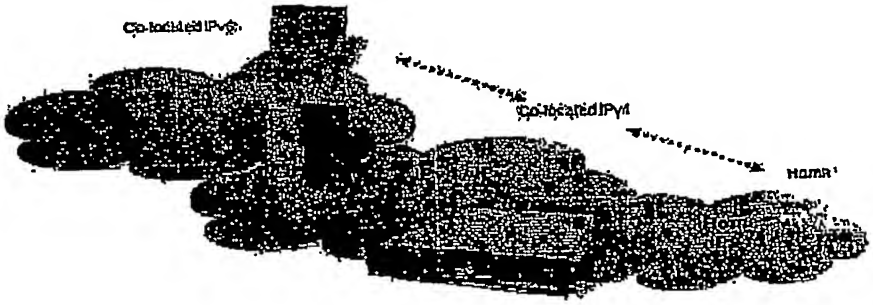


Figure 6.1: The test network setup.

6.3 Verification of Goals

Before the prototype was implemented a list of goals was set up. These goals was set as the minimum requirements for the prototype, any features outside of these goals was not to be focused on. Additional goals was set up for the Mobile Node in order to use Mobile IPv4 over IPv6 without the IPv6 stack installed in Microsoft Windows 2000/XP.

6.3.1 Home Agent

The following list presents the goals set up for the prototype implementation of the Home Agent and the resulting functionality achieved by the implementation.

1. **The Home Agent has to be extended to handle Registration Requests over IPv6.**
   Result: The Home Agent successfully handles Registration Requests over IPv6.

2. **The Home Agent has to be able to send Registration Replies to the Mobile Node over IPv6.**
   Result: The Home Agent sends Registration Replies to the Mobile Node over IPv6, informing the Mobile Node of the result of the registration.

3. **The Home Agent has to handle the new IPv6 Care-of Address Extension in Registration Requests.**
   Result: The Home Agent parses the Registration Request and identifies the IPv6 Care-of Address Extension and uses this address as the Care-of address for the Mobile Node.

4. **The Home Agent has to be able to decapsulate IPv6 tunneled IPv4 packets from the Mobile Node.**
   Result: The Home Agent successfully decapsulate IPv6 tunneled IPv4 packets and sends them to the correct destination.

5. **The Home Agent has to be able to encapsulate IPv4 packets in the IPv6 tunnel.**
   Result: The Home agent successfully encapsulates IPv4 packets in the IPv6 tunnel.

6.3.2 Mobile Node

The following list presents the goals set up for the prototype implementation of the Mobile Node and the resulting functionality achieved by the implementation.

1. **The Mobile Node has to be able to receive router advertisements with prefix information, in order to configure the IPv6 address to use. The IPv6 address has to be configured using the stateless address auto-configuration method.**
   Result: The Mobile Node successfully receives router advertisements and parses out the prefix information. This prefix information is then used to configure the IPv6 address according to the method used in stateless address auto-configuration. However, when no IPv6 protocol is installed, sometimes the client does not receive router advertisements and neighbor discovery messages. The reason for this is that Windows registers a new multicast MAC address list that does not contain the necessary MAC addresses for reception of router advertisements and neighbor discovery messages. The workaround

for this problem is to pull the network cable and put it back in, this triggers the driver to register the multicast MAC address list again.

2. **The Mobile Node has to be able to send Registration Requests over IPv6, using the configured IPv6 address as source address, and the Home Agent IPv6 address as destination address.**
Result: The Mobile Node sends Registration Requests over IPv6 once the IPv6 care-of address has been configured. The Home Agent IPv6 address is retrieved from the configuration of the client.

3. **The Mobile Node has to be able to include the IPv6 Care-of Address Extension in the Registration Request.**
Result: The Mobile Node attaches the IPv6 Care-of Address Extension to the Registration Request when Co-located on IPv6.

4. **The Mobile Node has to be able to encapsulate IPv4 packets in IPv6 headers, destined for the Home Agent.**
Result: The Mobile Node successfully encapsulates outgoing IPv4 packets in IPv6 headers.

5. **The Mobile Node has to be able to decapsulate IPv6 tunneled IPv4 packets from the Home Agent.**
Result: The Mobile Node successfully decapsulates IPv6 tunneled IPv4 packets and sends them up to the virtual adapter.

6. **The Mobile Node has to be able split tunnel IPv6 traffic, i.e. IPv6 traffic should be sent directly out on the interface and not tunneled to the Home Agent. This allows the use of IPv6 services at the same time as IPv4 mobility is used from an IPv6 access network.**
Result: IPv6 split tunneling is working correctly. It is however not possible to turn this feature off.

The additional goals set up for the Mobile Node was also implemented. The additional goals and the resulting functionality are presented below:

1. **The Mobile Node should be able to notify the network interface driver to receive the necessary multicast traffic in order to receive router advertisements and neighbor solicitations. This is something that the IPv6 driver normally does, but as IPv6 will not be installed, the Mobile Node has to do it.**
Result: The Mobile IP driver registers a multicast MAC address list with the network interface driver for reception of traffic sent to the special multicast MAC addresses used in router advertisements and neighbor solicitations. This is currently only done whenever the driver recognizes link-up, i.e. when the network cable is connected.

2. **The Mobile Node should be able to respond to neighbor solicitations. In order for the Mobile Node to behave as an IPv6 node among other nodes in the network, the Mobile Node should fully support Neighbor Discovery, but for a minimal prototype implementation it is enough to respond to neighbor solicitations. Neighbor solicitations are sent as a query to get the MAC address of the node, if the Mobile Node does not respond to these solicitations, IPv6 packets from the IPv6 router in the network cannot be sent to the Mobile Node.**
Result: The Mobile Node can receive neighbor solicitations and send out neighbor advertisements to solicitating nodes.

BEST AVAILABLE COPY

6.4 Performance

The performance of the Mobile IPv4 over IPv6 solution when co-located on IPv6 has been measured and compared to co-located on IPv4. The performance of the prototype implementation is not in any case representable of the performance of ipUnplugged's Mobile IP solution, due to the extensive changes in the code and the quality of the test network. To start with, we can theoretically calculate how big the relative performance decrease should be when co-located on IPv6.

If we assume that the IPv6 routing is as fast as IPv4 routing, we know that the IPv6 header is 40 bytes compared to the IPv4 header of 20 bytes. This gives an additional overhead of 20 bytes per packet for the Mobile IPv4 over IPv6 solution. If each packet is 1500 bytes, this gives a performance loss of transferred data at about 1.33%. However, one must also take into account the performance cost of the addition of an IPv6 stack in the Roaming Gateway, and the new larger data structures used to hold IPv4 and IPv6 addresses in the Mobile IP implementation on the Roaming Gateway, as well as the new data structures used in the Roaming Client. This cost is difficult to calculate, therefore some basic performance testing has been done.

6.4.1 Evaluation Method

The performance of the prototype was evaluated using the TPTEST [TPTEST] server version 3.10 and client version 3.0.10. The TPTEST server is running on the IPv6 router in the test network, and the TPTEST client is running on Windows on the Mobile Node. The tests were performed in a 10 Mbit/s network consisting of two laptops and a Roaming Gateway, where one laptop was used as Mobile Node and one as IPv4/IPv6 router. The router is connected to the Roaming Gateway through a 10 Mbit/s hub. Tests were done while registered Co-located behind the router on IPv4 and IPv6, with IPsec turned off. One test consisted of transmission and reception of five megabyte of data to and from the TPTEST server using the TCP protocol with standard settings in TPTEST. The test was repeated 10 times for each type of access method, totalling to 20 test runs during the evaluation phase.

6.4.2 Results

The results of the test runs showed that Co-located on IPv6 using Mobile IPv4 over IPv6 has minimal performance loss over Co-located on IPv4. The measured performance loss when Co-located on IPv6 compared to Co-located on IPv4 was only 0.25% when sending data, and 1.32% when receiving data. The measured results are very close to the theoretical calculation, and should be barely noticeable for the user.

If time allowed, a more extensive evaluation of the performance could have been done, with less bottlenecks in the network such as hubs and old 10 Mbit/s network interfaces. However, due to time constraints such an evaluation could not be done.

6.5 Usability

As the implementation of the Mobile IPv4 over IPv6 solution was aimed towards a prototype, the focus has not been to make the Roaming Client and Gateway as user friendly as possible. However, the usability of the solution is quite good for a prototype.

6.5.1 Roaming Client

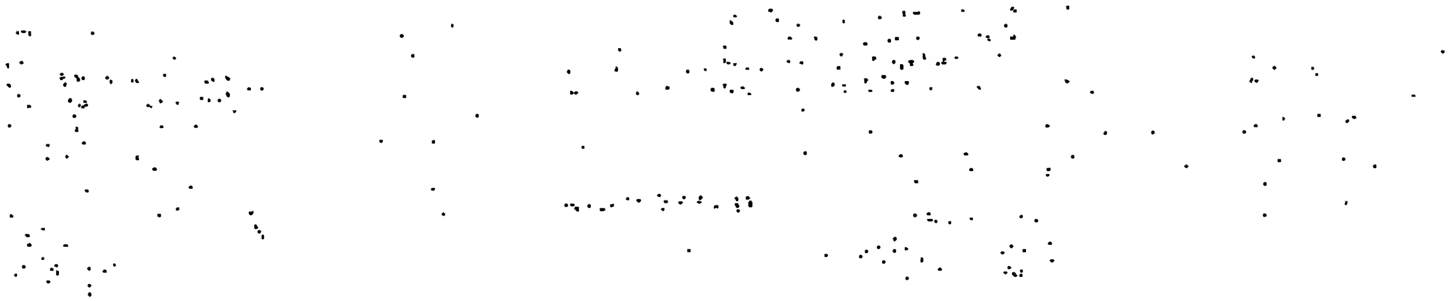
If the client is configured correctly, i.e. configured with the IPv6 address of the Home Agent, then seamless roaming between IPv4 and IPv6 access networks is as easy as switching network cables or moving around in the office between different access points. The user does not need to be aware of the type of access network as the transition is transparent to the user. It is possible to get details about the currently used Care-of address, Home Agent etc, in the configuration dialog of the control application. If no IPv6 applications are used, then it is not needed to install the IPv6 stack in Windows, as the client can operate on IPv6 networks without the Windows IPv6 stack. However, if the user wants to use IPv6 programs, all that needs to be done is to install the IPv6 stack by typing the "ipv6 install" command in a console. This only works on Windows XP with SP1 or never.

6.5.2 Roaming Gateway

The Roaming Gateway needs manual configuration in order to work correctly. Due to time constraints the configuration of IPv6 addresses on the interfaces was not implemented as a part of the normal configuration method of the Roaming Gateway. Normally IP addresses can be assigned to interfaces using a CLI command, or via the web-based Roaming Server. To manually configure the IPv6 addresses to interfaces, root shell access on the Roaming Gateway is needed. In the shell the ifconfig and route commands are used to set IPv6 addresses and configure default routes.

6.6 Conclusions

The overall conclusion of the evaluation of the prototype is that it works as expected. The prototype is quite easy to install and use, but it could need some enhancements in the configuration of the Roaming Gateway. The performance of the prototype is relatively good considering no performance enhancements have been made.



Chapter 7

Conclusion

In this chapter I will summarize the work done during the master thesis and present the most important results. I will also present interesting work experiences gathered during the 20 weeks. Lastly, eventual further work will be suggested.

7.1 Summary

I have during this master thesis, on the behalf of ipUnplugged, proposed and implemented a solution for Mobile IPv4 that allow mobile users to maintain IPv4 mobility while seamlessly and securely roaming between access networks using different versions of the Internet protocol. The method developed is called Mobile IPv4 over IPv6. The implementation of the prototype was based on ipUnplugged's solution for IPv4 mobility, and the Roaming Gateway and Roaming Client was enhanced to support the Mobile IPv4 over IPv6 solution. The prototype can demonstrate seamless hand-over between IPv4 and IPv6 access networks, while maintaining IPv4 mobility for the user.

I have evaluated the prototype in practical tests in a network lab and it shows good performance in comparison with normal Mobile IPv4. The usability of the installation and usage of the client is very good, it is not necessary to install any IPv6 stack to use the new solution and the user does not need to be aware of which Internet protocol is currently used as hand-overs between access networks are totally seamless and free of manual configuration for the user.

7.2 Discussion

The next generation Internet protocol, IPv6, is by many believed to be a key component of the next generation of cellular networks. This is probably due to the vast amount of handheld IP devices that are expected to be used throughout the world once the next generation of cellular networks are started to be deployed. The reason for the expected amount of devices is the increased performance of the next generation cellular networks that allow transportation of data at a much higher rate than previously ever possible. The handheld devices can use more appealing services with a high speed data connection, such as high quality video conferencing, high speed Internet access etc. With these new possibilities it is likely that the new cellular networks are going to be used as access networks for mobile users that need a high speed Internet connection while on the move. Some of these mobile users are going to need the possibility to securely access their home network to use services such as mail servers, file storage etc. However, Mobile IPv4 that is used to achieve IPv4 mobility does not work when the user is connected to an IPv6 access network. As previously discussed in this thesis, there are solutions where Mobile IPv6 can be used to achieve IPv4 mobility from IPv6 access networks, and together with Mobile IPv4 this will allow seamless mobility between access networks using different versions of the Internet protocol. But it is not likely that IPv6 will be used in the home networks until the range of commercial applications supporting IPv6 is big enough and users feel the need to use IPv6. For this reason, I believe that users are not going to invest money in Mobile IPv6 solutions until IPv6 is actually used in the home network.

The Mobile IPv4 over IPv6 solution proposed in this master thesis, can be used to get IPv4 mobility from IPv6 access networks without the need for investments in Mobile IPv6 infrastructure. The solution is relatively easy to implement for Mobile IP vendors, compared to the work needed to implement a full Mobile IPv6 solution with support for IPv4 in Mobile IPv6. This will keep the cost down for companies and vendors and will allow use of IPv4 mobility from the next generation access networks using IPv6. However, as soon as IPv6 is deployed in home networks and applications and services in these networks are starting to use IPv6, investments in Mobile IPv6 solutions are needed to support IPv6 mobility. When IPv6 and Mobile IPv6 is used in the home environment and all hosts are dual stacked, there is no longer any need for Mobile IPv4 over IPv6. Instead it is preferable to use IPv4 over Mobile IPv6 as this solution can take advantage of the new features in Mobile IPv6.

To conclude, I believe Mobile IPv4 over IPv6 is a good solution to use during the period when IPv6 access networks are available, but home networks are still using IPv4 as the main network protocol for the internal services. I also believe that a solution like this can help to speed up the deployment of IPv6 in access networks and the acceptance of IPv6 in general, as it allows mobile users to fully take advantage of the next generation cellular networks and gradually get acceptance for IPv6 and to finally replace IPv4 in the home network as well.

7.3 Work Experiences

Before this master thesis I had no worries about the implementation on OpenBSD in the Home Agent, instead I believed that the risky part of the master thesis was the Mobile Node implementation on Microsoft Windows, as I have never developed drivers in Windows before. However, the implementation turned out well on both the Home Agent and Mobile Node. I got help from people at ipUnplugged whenever I had questions regarding their implementation of the Mobile Node and Home Agent. Without their support I do not believe that the prototype would have ended up to be as successful as it did.

During development of the new functionality in the Home Agent and Mobile Node, I have gathered knowledge in programming of large scale applications. Applications can easily become very complex and it is important to stay to the chosen architecture and not cut any corners that you will end up regretting in the future. The importance of good tools for debugging are not to be underestimated, especially when it comes to kernel development, both *BSD development and driver development in Microsoft Windows.

7.4 Further Work

There are still a lot of work do be done in order to get a release quality version of the Mobile IPv4 over IPv6 solution. To start with, the Roaming Client has to support different mechanisms for configuration of the IPv6 care-of address to use in access networks. Additional mechanisms that should be supported are Stateful Address

Auto-configuration and DHCPv6. If the client is supposed to work behind a NAT-PT gateway, some fundamental changes have to be made to the client. First the client has to configure its IPv6 care-of address using DHCPv6 as the IPv6 address of the local DNS server is needed. Next, before trying to register with the Home Agent, the Mobile Node has to look up the IPv6 address of the Home Agent by sending a DNS request for the IPv6 address configured to the domain name of the Home Agent. When the IPv6 address is retrieved, the Mobile Node can send the Registration Request as usual.

The Home Agent has to be secured by an IPv6 firewall. The Roaming Gateway has a built in IPv4 firewall that has to be IPv6 enabled and easily configurable with IPv6 firewall rules. It should also be made as easy to configure IPv6 addresses on the interfaces in the Roaming Gateway as it is to configure IPv4 addresses.

Bibliography

[IETF] Internet Engineering Task Force, IETF, http://www.ietf.org

[IPv4] Information Sciences Institute, University of Southern California, "Internet Protocol", RFC 791, September 1981.

[NAT] K. Egevang, P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.

[IPv6] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6)", RFC 2460, December 1998.

[IPsec] IP Security Protocol (ipsec), http://www.ietf.org/html.charters/ipsec-charter.html

[DoCoMo] NTT DoCoMo 4G network, http://www.nttdocomo.co.jp/corporate/rd/new_e/4gen01_e.html

[ngtrans] Next Generation Transition, IETF working group, http://www.ietf.org/html.charters/ngtrans-charter.html

[6to4] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[NAT-PT] G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[SIIT] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.

[TRT] J. Hagino, K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator", RFC 3142, June 2001.

[BIA] S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)", RFC 3338, October 2002.

[DSTM] Jim Bound, "Dual Stack Transition Mechanism", draft-bound-dstm-exp-00.txt, August 2003.

[Dual-MIPv4] G. Tsirtsis, H. Soliman, "Dual Stack Mobile IPv4", draft-tsirtsis-v4v6-mipv4-00.txt, August 2003.

[Dual-MIPv6] H. Soliman, G. Tsirtsis, "Dual Stack Mobile IPv6", draft- soliman-v4v6-mipv4-00.txt, August 2003.

[IPv6-MIPv4] Pat R. Calhoun, Paal E. Engelstad, Tom Hiller, Peter J. McCann, "IPv6 over Mobile IPv4", draft-mccann-mobileip-ipv6mipv4-03.txt, October 2002.

[MIPv4] C. Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002.

[MIPv6] D. Johnson, C. Perkins, j. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt, June 2003.

[RFC2462] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3519] H. Levkowetz, S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, April 2003.

[RFC3115] G. Dommety, K. Leung, "Mobile IP Vendor/Organization-Specific Extensions", RFC 3115, April 2001.

[Ethereal] Ethereal Network Protocol Analyzer, http://www.ethereal.com

[TPTEST] TPTEST, The Internet Bandwidth Tester, http://tptest.sourceforge.net